Notice of Allowability	Application No.	Applicant(s)	
	09/643,630	SIBERT, W. OLIN	
	Examiner	Art Unit	
	Kyung H. Shin	2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *5/26/06*.

2. ☒ The allowed claim(s) is/are *1-5, 10-14 and 18*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

DETAILED ACTION

1. This action is responding to application amendment dated 5/26/2006.

2. Claims **1 - 5, 10 - 14, 18** are pending. Claims **1, 10, 11** have been amended. **Claims 6 - 9, 15 – 17, 19 - 21** are **canceled** and incorporated into independent claims. Independent claims are **1, 11**.

EXAMINER'S AMENDMENTS

3. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Weiguo (Will) Chen: L.R. No. L0024 at 650-849-6729 on 7/31/2006.

4. The application has been amended as follows:

AMENDED CLAIMS 1, 10, 11 AND CANCELED CLAIMS 7, 8, 15, 16:

1. (Currently amended) A secure processing unit comprising:

an internal memory unit;

a processor;

tamper detection and response logic;

an interface to external systems or components;

one or more buses for connecting the internal memory unit, the processor, the tamper detection and response logic, and the interface to external systems and components;

a memory management unit;

a level-one page table, the level-one page table including a plurality of level-one page table entries, wherein the level-one page table entries each correspond to at least one level-two page table, and wherein the level-one page table entries each contain a predefined attribute, the predefined attribute being operable to indicate to the memory management unit whether entries in a corresponding level-two page table may designate certain predefined memory regions;

a plurality of processor security registers;

access control data, the access control data being operable to indicate whether access to predefined memory regions is restricted to certain software components or processor modes, wherein the access control data are stored in a critical address register, the critical address register comprising one of the processor security registers; and

a tamper-resistant housing.

2. (Original) A secure processing unit as in claim 1, in which the internal memory unit includes:

secure random access memory;

secure non-volatile memory;

secure read-only memory.

3. (Original) A secure processing unit as in claim 2, in which the secure non-volatile memory is powered by a battery.

4. (Original) A secure processing unit as in claim 3, in which the secure non-volatile memory contains at least one cryptographic key.

5. (Original) A secure processing unit as in claim 1, in which the internal memory unit includes a unique identifier for the secure processing unit, a private cryptographic key, a public cryptographic key, and a cryptographic certificate linking the unique identifier and the public cryptographic key.

6. (Canceled)

7. (Canceled)

8. (Canceled)

9. (Canceled)

10. (Currently amended) A secure processing unit as in claim 1, whereby level-two page tables that ~~may not~~ designate the predefined memory regions are ~~not~~ stored in the internal memory unit.

11. (Previously Presented) An information appliance comprising:

a memory unit;

a secure processing unit comprising:

a tamper resistant packaging,

tamper detection and response logic,

a secure memory unit, ~~and~~

a processing unit, including a memory management unit and a plurality of processor security registers; and

access control data, the access control data being operable to indicate whether access to predefined memory regions is restricted to certain software components or processor modes, wherein the access control data are stored in a critical address register, the critical address register comprising one of the processor security registers;

a level-one page table and a plurality of level-two page tables, the level-one page table including a plurality of level-one page table entries and the level-two page table including a plurality of level-two page table entries, wherein the level-one page table entries each correspond to at least one level-two page table, and wherein the level-one page table entries each contain a predefined attribute, the predefined attribute being operable to indicate to the memory management unit whether a corresponding level-two page table may designate certain predefined memory regions; and

a bus for connecting the memory unit and the secure processing unit;

wherein the secure processing unit is operable to perform both secure processing operations and at least some processing operations performed by a conventional information appliance processing unit.

12. (Original) An information appliance as in claim 11, in which the information appliance is selected from the group comprising: a television set-top box, a portable audio player, a portable video player, a cellular telephone, a personal computer, and a workstation.

13. (Original) An information appliance as in claim 11, in which the secure processing unit is the information appliance's primary processing unit.

14. (Original) An information appliance as in claim 11, in which the secure processing unit is the information appliance's only processing unit.

15. (Canceled)

16. (Canceled)

17. (Canceled)

18. (Previously Presented) An information appliance as in claim 11, in which level-two page tables that may not designate the predefined memory regions are stored in the memory unit, and wherein the level-one page table and the level-two page

tables that may designate the predefined memory regions are stored in the secure memory unit.

19 - 21. (Canceled)

Allowable Subject Matter

5. The following is an examiner's statement of reasons for allowance:

Applicant discloses in Independent claims **1** and **11,** Secure Processing Unit systems. After extensive searching and analysis of prior art in light of the Applicant's claimed invention, the examiner finds that the referenced prior art does not teach or suggest in detail that memory management unit utilizes level-one page table and level-two page tables, where A level-one page table entries contain an attribute indicates, whether an entry in a corresponding level-two page table designates certain memory regions, as of the invention's disclosure in combination with all the elements of each independent claim as argued by the Applicant.

So as indicated by the above statements, Applicant's arguments have been considered persuasive, in light of the claim limitations as well as the enabling portions of the specification. The dependent claims, **2-5, 10, 12-14, 18,** further limit the independent claims and are considered allowable on the same basis as the independent claims as well as for the further limitations set forth.

6. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kyung H. Shin whose telephone number is (571) 272-3920. The examiner can normally be reached on 7:30 am - 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David A. Wiley can be reached on (571) 272-3923. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KHS
Kyung H Shin
Patent Examiner
Art Unit 2143

KHS
8/4/2006

DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100